(19) BUNDESREPUBLIK DEUTSCHLAND

DEUTSCHES PATENT- UND MARKENAMT

(12) **Offenlegungsschrift**

(10) **DE 100 65 907 A 1**

(51) Int. Cl.[7]: G 06 F 11/08

(21) Aktenzeichen: 100 65 907.1
(22) Anmeldetag: 29. 11. 2000
(43) Offenlegungstag: 26. 9. 2002

(71) Anmelder:
Gall, Heinz, 53881 Euskirchen, DE; Wratil, Peter, Dr., 21224 Rosengarten, DE

(72) Erfinder:
gleich Anmelder

Die folgenden Angaben sind den vom Anmelder eingereichten Unterlagen entnommen

Prüfungsantrag gem. § 44 PatG ist gestellt

(54) Verfahren zum gesicherten Datentransport

(57) Es wird ein Verfahren beschrieben mit dem man sicherheitsrelevante Daten über ein ungesichertes Medium transportieren kann. Das Verfahren ist derart ausgelegt, dass nahezu alle statistischen und systematischen Fehler des gesamten Übertragungssystems keine negative Auswirkung auf die Sicherheit der Übertragungsdaten haben. Durch das Verfahren wird ein Empfänger einer Nachricht in die Lage versetzt, die empfangene Dateninformation auf Richtigkeit zu überprüfen und damit allle möglichen Fehlerfälle während der Übertragung zu erkennen. Sofern der Empfänger eine Fehler (oder mehrere Fehler) erkennt, kann er die Dateninformation erneut anfordern oder in einer geeigneten Art und Weise reagieren.

DE 100 65 907 A 1

DE 100 65 907 A 1

Beschreibung

[0001] Die Übertragung sicherheitsrelevanter Daten hat in den letzten Jahren erheblich an Bedeutung zugenommen. Dies ist insbesondere dadurch gekommen, dass elektronische Verfahren nach und nach mechanische oder elektromechanische Sicherheitseinrichtungen ersetzen. Diese modernen elektronischen Verfahren bringen dabei einen erheblich verbesserten Sicherheitsanteil mit sich und erhöhen gleichfalls den Komfort der betreffenden Maschine oder Anlage.

[0002] Die elektronischen Sicherungsverfahren verwenden dabei nicht selten Bussysteme, die Daten von Sensoren, Aktoren und Steuerungseinrichtungen übertragen. Für alle sicherheitsrelevanten Applikationen ist es dabei unbedingt notwendig, dass alle Daten ohne irgend eine Verfälschung zeitgerecht transportiert werden. Jede Verfälschung kann eine fehlerhafte Funktion zur Folge haben, die in letzter Konsequenz das Leben und die Gesundheit von Personen gefährdet.

[0003] Um dieser Anforderung gerecht zu werden, hat es in den letzten Jahren zahlreiche Vereinbarungen gegeben, die einen nahezu fehlerfreien Datentransport beim Einsatz von Bussystemen fordern. Nicht zuletzt sind in den internationalen Normen Festlegungen getroffen worden, wie man Daten zu transportieren hat und welcher Restfehler noch erträglich ist. Die zulässige Restfehlerwahrscheinlichkeit orientiert sich dabei an der Anwendung, die eventuell eine Gefahr für die Person darstellt (siehe DIN V VDE 0801, EN **954-1** oder IEC 61508).

[0004] Entsprechend dieser Vereinbarungen und Normen sind sicherheitsgerichtete Bussysteme entwickelt worden, die Daten mit hoher Redundanz übertragen. Mögliche Fehler werden rechtzeitig entdeckt und eine Gefährdung kann abgewendet werden (Beispiele: Safety Bus P, Profibus F, Interbus Safety, u. a.).

[0005] Mit dem Einsatz der vorher genannten sicherheitsgerichteten Bussysteme entstehen für den Anwender jedoch einige Nachteile, die oftmals nicht in Kauf genommen werden können. So müssen eventuell bereits installierte Bussysteme durch die Sicherheitsbusse ersetzt werden. Zusätzlich bringen nahezu alle Sicherheitsbussysteme spezielle Einschränkungen bei der Anzahl der Teilnehmer, bei der Datentransportrate oder beim Datenprotokoll mit sich.

[0006] Das in dieser Erfindung vorgeschlagene Verfahren verwendet eine vollkommen andere Technik. Es ist derart ausgelegt, dass man sicherheitsrelevante Daten auch über normale Bussysteme transportieren kann, ohne einen fatalen Fehler in Kauf nehmen zu müssen.

[0007] Das Prinzip dieser Erfindung beruht darauf, dass man die Daten vor dem Versenden mit einer geeigneten Redundanz versieht, die den Empfänger in die Lage versetzt alle denkbaren Fehler mit absoluter Sicherheit zu erkennen. Dieses gilt nicht nur für statistische Fehler (wie Störungen, elektrische Einflüsse, usw.) sondern auch für alle systematischen Fehler (wie z. B.: Falscher Aufbau bestimmter Strukturen in der Hardware oder Programmierfehler) im Übertragungsmedium bzw. den Interface-Einheiten. Der Einsatz sicherheitsgerichteter Bussysteme ist damit nicht mehr notwendig.

[0008] Wie die **Fig.** 1 zeigt, stellt die Applikation auf der Sensor-Seite eine Information zur Verfügung (**1**). Es geht nun darum, diese Information sicher zu einem Empfänger (z. B.: zu einem Aktor zu übertragen). Das hier gewählte Beispiel kann auf alle anderen Übertragungseinheiten umgesetzt werden (z. B.: Speicherprogrammierbare Steuerungen, Überwachungseinheiten, intelligente Lichtgitter oder Antriebe). Es hängt von der Art der Applikation ab, ob die Dateninformation von der Applikationsseite (**1**) zweikanalig

zur Verfügung steht. Dieser Teil ist insbesondere nicht Bestandteil der Erfindung und daher nur zum besseren Verständnis eingezeichnet. Die Applikationsseite versorgt 2 vollkommen unabhängige Mikroprozessoren oder ähnliche Einheiten (z. B.: FPGAs) (**2, 3**) mit den relevanten Sicherheitsdaten der Peripherie (**1**). Beide Mikroprozessoren (**2, 3**) bereiten diese Daten unabhängig auf, so dass sie als Transport-Größe über den Bus verschickt werden können. Neben der reinen Dateninformation fügen beide Mikroprozessoren (**2, 3**) eine hochwertige Redundanz hinzu. Diese Redundanz garantiert eine hohe Hamming-Distanz. Jede spätere Verfälschung von einem Datum oder mehreren Daten in jedem der beiden Transport-Blocks wird dadurch mit hoher Sicherheit erkannt.

[0009] Vor dem eigentlichen Datentransport tauschen beide Mikroprozessoren (**2, 3**) ihre Daten inklusive der redundanten Information aus und vergleichen diese gegenseitig auf Übereinstimmung (**4**). Sofern beide zum gleichen Ergebnis gelangt sind, übergibt jeder der Mikroprozessoren seinen Übertragungsdaten einem Zwischenregister (**8**). Das Zwischenregister besteht damit aus den beiden Bestandteilen (**9**) und (**10**), die von den beiden Mikroprozessoren mittels eines Datentransfers (**5, 6**) erzeugt werden.

[0010] Dieses Zwischenregister kann auch Bestandteil eines der Mikroprozessoren sein (z. B.: ein internes Register des Mikroprozessors (**2**)). In diesem Fall erzeugt der Mikroprozessor (**2**) beide getrennten Bestandteile nach der Abstimmung mit dem Mikroprozessor (**3**). Zur Kontrolle liest der zweite Mikroprozessor (**3**) das Zwischenregister (**8**) mit den beiden Bestandteilen (**9**) und (**10**) nochmals aus (gestrichelter Pfeil (**7**)). Je nach Applikation kann der Dateninhalt eines der beiden Bestandteile (**9**) und (**10**) des Zwischenregisters (**8**) auch invertierte Daten oder andere zusätzliche Verschachtelungen aufweisen. Das Zwischenregister (**8**) kann auch ein Bestandteil der nachfolgenden Interface-Einheit (**11**) sein. Der konkrete Aufbau hängt dabei von der benutzten Technologie ab.

[0011] Das Zwischenregister (**8**) stellt damit den eigentlichen Kern der Erfindung dar. Es enthält zwei logisch identische Datenbereiche (**9**) und (**10**), die ihrerseits bereits redundante Daten zur Fehlererkennung enthalten. Das Zwischenregister (**8**) stellt in der Summe seines Dateninhalts ein hochredundantes System dar, das auch bei mehrfacher Verfälschung sofort jeden möglichen Fehler sichtbar machen kann.

[0012] Vom Zwischenregister gelangt die gesamte Dateninformation über das Interface (**11**) zum Bussystem (**12**). Das Interface (**11**) besteht in der Regel aus mehreren logischen Funktionen, die je nach Anwendung durch Hard- oder Software realisiert sind. Das Bussystem (**12**) kann sowohl aus einem parallelen oder seriellen Bussystem bestehen, welches die Daten überträgt. In der **Fig.** 1 ist das Beispiel eines seriellen Bussystems gewählt, wie es z. B. beim Profibus oder beim Ethernet bekannt ist.

[0013] Über das Bussystem (**12**) nimmt nun das Datenpaket entsprechend der Datenstruktur nach der Zuordnung des Zwischenregisters (**8**) seinen Weg. Hier kann das Datenpaket durch Verstärker, Switches, Gateways, Bridges oder andere Einrichtungen verfälscht werden (**13**). Zusätzlich besteht die Möglichkeit, dass die Daten während des Transports durch äußere Einwirkungen (**14**) verfälscht werden. Freilich kann auch das Interface (**11**) selbst Fehler aufweisen oder erzeugen. Diese Einwirkungen können elektromagnetische Einflüsse oder sonstige statistische Einwirkungen sein.

[0014] Auf der Empfangsseite wird das Datenpaket von dem Interface (**15**) des Empfängers entgegengenommen und wieder vollständig in einem Zwischenregister (**16**) abgelegt.

Hier gelangen die beiden Datenbereiche (9) und (10) der Senderseite in die Datenbereiche (17) und (18) des Zwischenregisters (16).

[0015] Die beiden Mikroprozessoren (19) und (20) nehmen jeweils das für sie bestimmte Datenpaket (17 für Mikroprozessor 19) und (18 für Mikroprozessor 20) entgegen. Beide Mikroprozessoren (19, 20) überprüfen das jeweilige Datenpaket auf Richtigkeit, indem sie die Redundanz des jeweiligen Datenpakets untersuchen. Sofern beide Mikroprozessoren (19, 20) die Richtigkeit überprüft haben, vergleichen sie die Dateninhalte direkt (21). Bei erneuter Übereinstimmung können die Mikroprozessoren (19, 20) die reinen Nutzdaten (ohne die Redundanz) an die Peripherie (z. B. an einen Aktor) weitergeben.

[0016] Das Verfahren zeigt eine besonders große Immunität gegenüber Störungen. Dabei spielt es keine Rolle, ob die Störungen systematische Natur (z. B. wie bei 13) oder statistischer Natur (z. B. wie bei 14) sind. Die Wirkung des Verfahrens beruht darauf, dass der Inhalt des Zwischenregisters (8) bei absolut richtiger Übertragung in das Zwischenregister (16) kopiert wird (23). Das Hinzufügen einer Redundanz für die beiden Datenbereiche (9) und (10), sowie die Verdopplung mit gegenseitigem Vergleich auf der Sende- (4) als auch auf der Empfangsseite (21) erlaubt es, jeden denkbaren Fehler zu erkennen. Für eine reale Implementierung sollte die Redundanz allerdings hinreichend hoch gewählt werden. Wenn man beispielweise jeden der Datenbereiche mit einer Hamming-Distanz von 4 versieht, entsteht ein gesamter Datenblock mit einer Hamming-Distanz von 8. Es ist ebenfalls angeraten, zusätzliche Maßnahmen bei der Datenerzeugung zu unternehmen, die Ausfälle im System selbst erkennen. Zu diesen Maßnahmen gehört beispielweise das Hinzufügen einer laufenden Nummer oder das Versenden von Adress-Informationen, sowie die Implementierung einer Zeiterwartung bei allen Empfängern. Eine Struktur in dieser Form lässt sich kaum durch irgendwelche Einwirkungen derart verändern, dass mögliche Fehler unerkannt bleiben.

[0017] Mit dieser Erfindung besteht im Prinzip die Möglichkeit, sicherheitsrelevante Daten über beliebige unsichere Medien zu übertragen, ohne dass die geforderter Sicherheit verloren geht. Für reelle Applikationen ergibt sich damit der entscheidende Vorteil, dass alle an der Datenübertragung beteiligten Einrichtungen weder besonders für die Sicherheitstechnik auszulegen sind, noch einer Überprüfung auf Fehlerfreiheit unterzogen werden müssen.

Patentansprüche

1. Verfahren zum gesicherten Datentransport für die Datenübertragung an parallelen oder seriellen Netzwerken oder Bussystemen (12), **dadurch gekennzeichnet**, dass ein Zwischenregister (8) verwendet wird, das hochredundante Daten enthält, dessen Inhalt über nahezu beliebige, auch unsichere Medien mit statistischen (14) oder systematischen Fehleranteilen (13), transportiert werden kann, ohne dass ein Verlust der Sicherheit entsteht, und der Inhalt des Zwischenregisters (8) auf der Senderseite auf ein Zwischenregister (16) der Empfangsseite kopiert wird (23), derart, dass über ein spezielles Verfahren mit redundanten Mikroprozessoren (2, 3, 19, 20) nahezu jeder Fehler aufgedeckt werden kann.

2. Verfahren nach dem Anspruch 1, dadurch gekennzeichnet, das der Inhalt des Zwischenregisters (8) auf der Senderseite durch 2 unabhängige Mikroprozessoren (2, 3) oder ähnliche Einrichtungen erzeugt wird, die eine von der Peripherie kommende Eingangsgröße (1) mit redundanten Daten versehen, diese gemeinsam und gegenseitig überprüfen (4) und dann die redundanten Daten über einen Datentransfer (5, 6) in Teilbereiche (9, 10) des Zwischenregisters (8) ablegen.

3. Verfahren nach den Ansprüchen 1 und 2, dadurch gekennzeichnet, dass die Empfangsseite ebenfalls ein Zwischenregister zur Verfügung stellt (16), das ebenfalls 2 Teilbereiche enthält (17, 18), die von den Mikroprozessoren (19, 20) ausgelesen werden, auf ihre Gültigkeit kontrolliert und dann in ihrem Dateninhalt gegenseitig ausgetauscht werden (21), damit nicht nur die Gültigkeit, sondern auch die tatsächliche Übereinstimmung der Information gewährleistet wird.

4. Verfahren nach den Ansprüchen 1 bis 3, dadurch gekennzeichnet, dass durch den speziellen Datentransfer mit der Hinzufügung von Redundanz eine direkte Kopie des Inhalts eines Zwischenregisters (8) von der Senderseite auf die Empfängerseite (16) entsteht.

5. Verfahren nach den Ansprüchen 1 bis 4, dadurch gekennzeichnet, dass eine Information von einer Senderseite (1), z. B.: einem Sensor oder einer Steuerung ohne Verlust an Sicherheit an den Ausgang (22) eines Empfängers z. B.: einem Aktor gelangt, auch wenn systematische (13) oder statistische (14) Verfälschungen vorliegen.

6. Verfahren, nach den Ansprüchen 1 bis 5, dadurch gekennzeichnet, dass die gesicherte Datenübertragung auch bei beliebigen Netzwerkinstallationen oder Interface-Einheiten (11, 15) erfolgen kann, ohne dass diese besonderen Maßnahmen zur Fehlerreduzierung unterzogen wurden.

Hierzu 1 Seite(n) Zeichnungen

Nummer: DE 100 65 907 A1
Int. Cl.[7]: G 06 F 11/08
Offenlegungstag: 26. September 2002

Figur 1